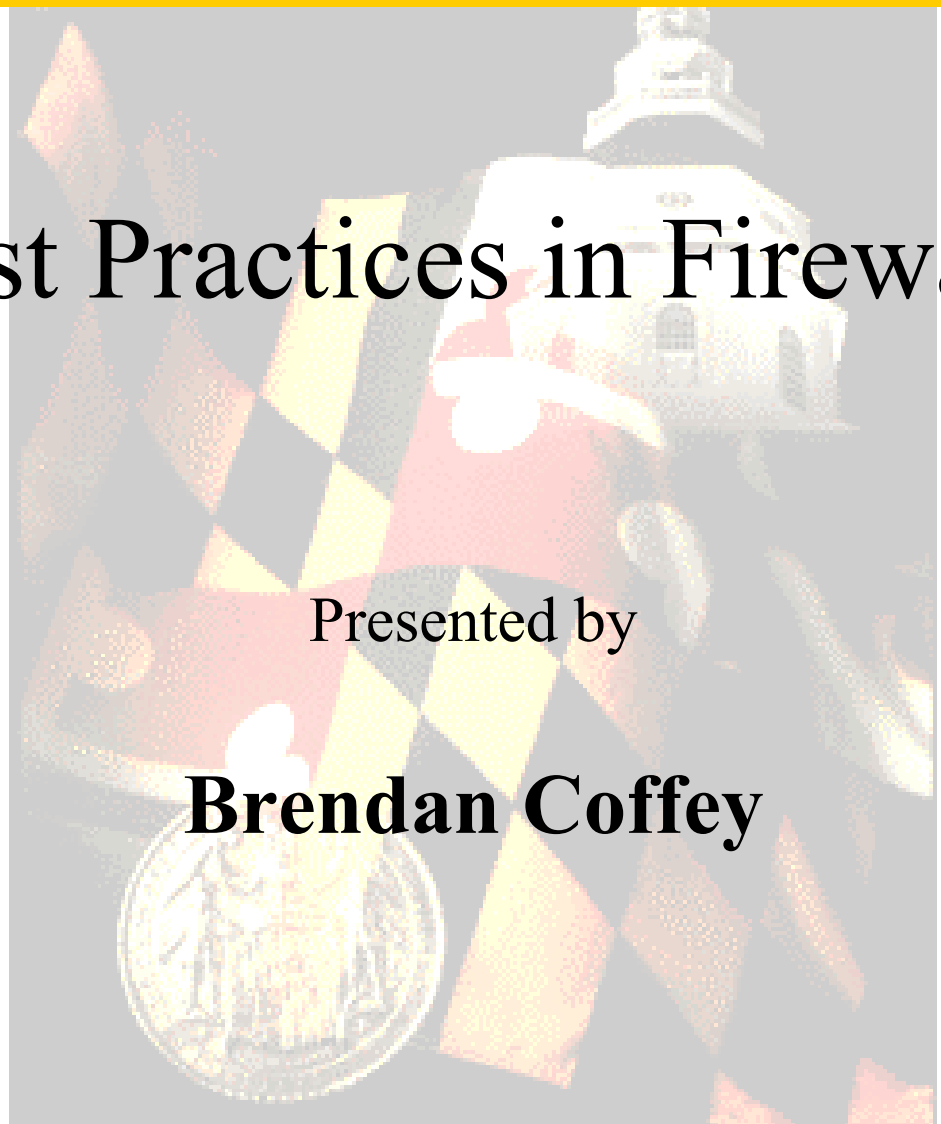
State of Maryland
IT Security and Privacy Conference



Best Practices in Firewalls

Presented by

Brendan Coffey

Firewall Best Practices

Outline

- Security Infrastructure
- Security Principles
- Firewall Overview
- Network Architecture
- Firewall Configuration
- Firewall Maintenance
- Additional Features
- Guidelines and Policies

Firewall Best Practices

Security Infrastructure

- Policies and Procedures
- Proper Equipment
- Device Placement and Network Segmentation
- Proper Security Settings
- Network Monitoring

Firewall Best Practices

Guiding Security Principles

- **Know Your Network**
  - What do you have available?
- **Least Privilege**
  - Access given on a “need to know” basis.
- **Defense in Depth**
  - Multiple lines of defense.
- **Detection is a Must**
  - Prevention is Ideal but Detection is a Must

Firewall Best Practices

Firewall Overview

- What is a firewall?
- Types of firewalls:
  - Packet Filter Firewall - the most basic firewall.
  - Stateful Inspection Firewall – Tracks sessions
  - Application-Proxy Gateway Firewall - advanced firewall that can filter at the application layer.

Firewall Best Practices

Network Architecture

- Placement of Firewall(s)
  - Which systems do we need to secure?
  - Where are the 3rd parties?
    - Internet Service Provider
    - Contractors, Agencies, Students
  - Do we need more than one firewall?

Firewall Best Practices

Network Architecture (Cont.)

- Service Network (DMZ)
  - Two types:
    - Traditional - Area separated by 2 firewalls.
    - Service Leg - one firewall with multiple network interfaces.
  - What goes in a DMZ?
    - Webservers, Email gateways, FTP servers

Firewall Best Practices

Firewall Configuration

- Firewall Rules
- Logging & Notification
- Administrative Management

Firewall Best Practices

Firewall Rules

- Comply with management's firewall policy.
- Follow the least privilege principle.
- Default should be a deny all rule.
- Keep it simple.
- Proper documentation or each rule.
- Keep them Updated

Firewall Best Practices

Logging & Notification

- Read your firewall's manual
- Log any dropped connection attempts.
- Log any firewall configuration modifications.
- Critical events should notify administrators

Firewall Best Practices

Firewall Administration

- Secure Remote Login Protocols
  - HTTPS – access with browser.
  - SSH – command prompt
  - Telnet/SSL – command prompt
- Strong Password Restrictions
- Who Knows the password(s)?
- Limit Source Locations

Firewall Best Practices

Firewall Maintenance

- Updates and Upgrades
- Log Storage & Review
- General Controls

Firewall Best Practices

Updates, Patches, & Upgrades

- Operating System and Application
- Written Procedures
- Research
  - Vendor websites
  - Other websites
- Follow vendor recommendations

Firewall Best Practices

Log Storage & Review

- Store Away from Firewall
  - removable media
  - Syslog server
- Proper Backup of logs
- Regular Review

Firewall Best Practices

General Controls

- Backup
- Physical Security
- Disaster Recovery

Firewall Best Practices

Additional Security Features

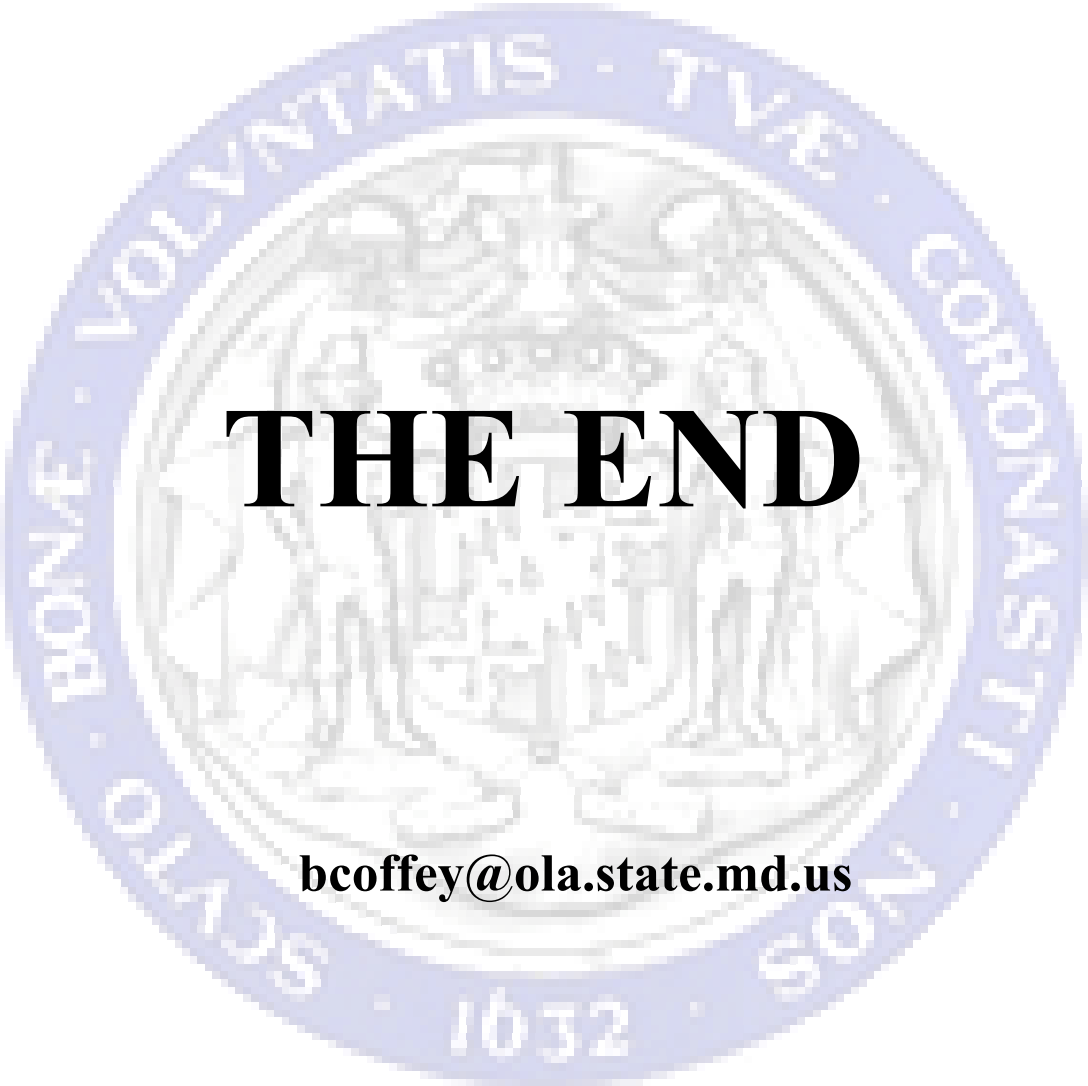
- Intrusion Detection System
- Traffic Content Scanning
- Anti-Spoof
- etc…

Firewall Best Practices

Guidelines & Policies

- National Institute of Standards and Technology (NIST)
  - Guidelines on Firewalls and Firewall Policy
- Dept. of Budget & Management
  - State Security Policy

Firewall Best Practices



THE END

bcoffey@ola.state.md.us